(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
27 janvier 2005 (27.01.2005)

PCT

(10) Numéro de publication internationale
WO 2005/008951 A3

(51) Classification internationale des brevets[7] : H04L 9/08, 9/30

(21) Numéro de la demande internationale :
PCT/FR2004/001362

(22) Date de dépôt international : 2 juin 2004 (02.06.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0307287 17 juin 2003 (17.06.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, Place d'Alleray, F-75015 PARIS (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **ARDITTI MODIANO, David** [FR/FR]; 46ter, rue Paul Vaillant-Couturier, F-92140 CLAMART (FR). **BILLET, Olivier** [FR/FR]; 1211 Route des Vallettes Sud, F-06140 TOURRETTES/LOUP (FR). **GILBERT, Henri** [FR/FR]; 2, allée des Peupliers, F-91440 BURES SUR YVETTE (FR).

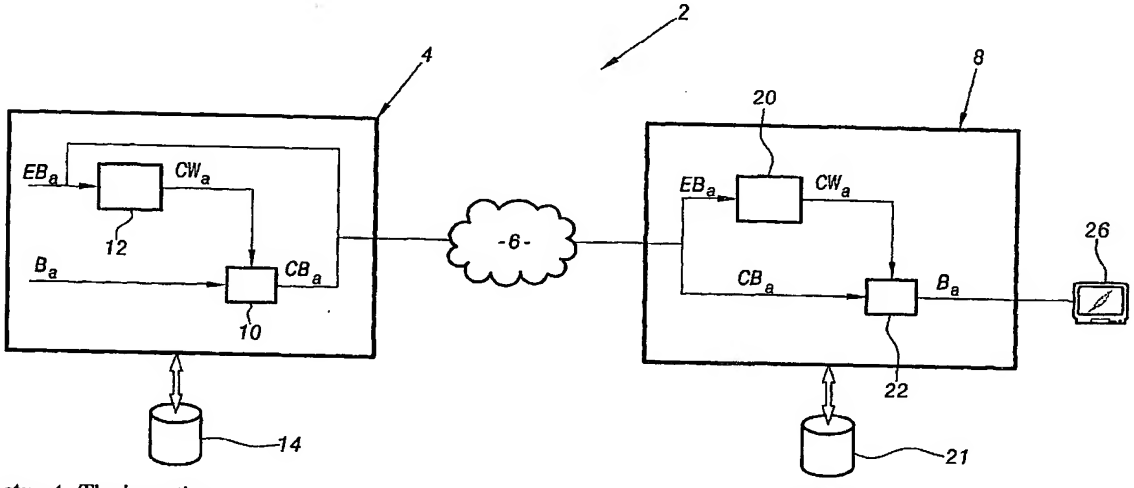
(74) Mandataires : **DOMENEGO, Bertrand** etc.; CABINET LAVOIX, 2, place d'Estienne d'Orves, F-75441 PARIS CEDEX 09 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,

[Suite sur la page suivante]

(54) Title: METHOD, SYSTEM AND MEDIA FOR RECORDING TRACEABLE ENCRYPTION AND/OR DECRYPTION

(54) Titre : PROCEDE, SYSTEME ET SUPPORTS D'ENREGISTREMENT DE CHIFFREMENT ET/OU DE DECHIFFREMENT TRAÇABLE



(57) Abstract: The invention concerns a non-combinatorial traceable method for encrypting and/or decrypting data broadcast by at least one transmitter towards several decoders not requiring the broadcast of a large number of encrypted headers, wherein: during encryption of broadcast data, the transmitter implements (in 86) at least one first secret function to transform an unencrypted message into an encrypted message; and during decryption of said broadcast data, all the decoders implement (in 92) at least one common second secret function, each decoder using therefor a mathematical description of the second function stored in a memory (21), the mathematical description of said second function being different from one decoder to another or from one group of decoders to another such that the mathematical description used identifies exclusively the particular decoder or group of decoders.

(57) Abrégé : L'invention concerne un procédé traçable non combinatoire de chiffrement et/ou de déchiffrement d'informations diffusées par au moins un émetteur vers plusieurs décodeurs ne nécéssitant pas la diffusion d'un nombre important d'en-têtes chiffrés, dans lequel : - lors du chiffrement des informations diffusées, l'émetteur met en œuvre (en 86) au moins une première fonction secrète pour transformer un message non chiffré

[Suite sur la page suivante]

WO 2005/008951 A3

CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

(88) **Date de publication du rapport de recherche internationale:** 3 novembre 2005

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

en un message chiffré, et - lors du déchiffrement de ces informations diffusées, tous les décodeurs mettent en œuvre (en 92) au moins une même seconde fonction secrète, chaque décodeur faisant appel à cet effet à une description mathématique de ladite seconde fonction enregistrée dans une mémoire (21), la description mathématique de cette seconde fonction étant différente d'un décodeur à l'autre ou d'un groupe de décodeurs à l'autre de manière à ce que la description mathématique à laquelle il est fait appel identifie de façon unique le décodeur ou un groupe de décodeurs particulier.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/001362

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
T	BILLET O, GILBERT H: "A Traceable Block Cipher" ASIACRYPT 2003: 9TH INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOLOGY AND INFORMATION SECURITY (SPRINGER-VERLAG, HEIDELBERG, LECTURE NOTES IN COMPUTER SCIENCE 2894), November 2003 (2003-11), pages 331-346, XP002273113 ISBN: 3-540-20592-6 the whole document	1-15

-/--

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 August 2005	24/08/2005

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer
Carmeniere, Rivero, F

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/001362

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BONEH D ; FRANKLIN M: "An efficient public key traitor tracing scheme" ADVANCES IN CRYPTOLOGY - CRYPTO'99. 19TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, 19 August 1999 (1999-08-19), pages 338-353, XP002273114 Santa Barbara, CA, USA ISBN: 3-540-66347-9 page 338 - page 343	1,2
A	MATSUMOTO T; IMAI H: "PUBLIC QUADRATIC POLYNOMIAL-TUPLES FOR EFFICIENT SIGNATURE-VERIFICATION AND MESSAGE-ENCRYPTION" ADVANCES IN CRYPTOLOGY- EUROCRYPT '88. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, PROCEEDINGS. SPRINGER VERLAG, DE, 1988, pages 419-453, XP000568374 ISBN: 3-540-50251-3 cited in the application the whole document	3-15
A	MENEZES; OORSCHOT; VANSTONE: "HANDBOOK OF APPLIED CRYPTOGRAPHY, PASSAGE" CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, 1997, pages 551-552, XP002273115 BOCA RATON, FL, USA ISBN: 0-8493-8523-7 page 551, paragraph 13.3.1 - page 552	1,2
A	PATARIN J ; GOUBIN L ; COURTOIS N: "Improved algorithms for isomorphisms of polynomials" ADVANCES IN CRYPTOLOGY - EUROCRYPT '98. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, 4 June 1998 (1998-06-04), pages 184-200, XP002273116 Espoo, Finland ISBN: 3-540-64518-7 the whole document	3-15

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR2004/001362

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/08 H04L9/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
T	BILLET O, GILBERT H: "A Traceable Block Cipher" ASIACRYPT 2003: 9TH INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOLOGY AND INFORMATION SECURITY (SPRINGER-VERLAG, HEIDELBERG, LECTURE NOTES IN COMPUTER SCIENCE 2894), novembre 2003 (2003-11), pages 331-346, XP002273113 ISBN: 3-540-20592-6 le document en entier ----- -/--	1-15

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
10 août 2005	24/08/2005

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Cammarano, A.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR2004/001362

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	BONEH D ; FRANKLIN M: "An efficient public key traitor tracing scheme" ADVANCES IN CRYPTOLOGY - CRYPTO'99. 19TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, 19 août 1999 (1999-08-19), pages 338-353, XP002273114 Santa Barbara, CA, USA ISBN: 3-540-66347-9 page 338 - page 343	1,2
A	MATSUMOTO T; IMAI H: "PUBLIC QUADRATIC POLYNOMIAL-TUPLES FOR EFFICIENT SIGNATURE-VERIFICATION AND MESSAGE-ENCRYPTION" ADVANCES IN CRYPTOLOGY- EUROCRYPT '88. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, PROCEEDINGS. SPRINGER VERLAG, DE, 1988, pages 419-453, XP000568374 ISBN: 3-540-50251-3 cité dans la demande le document en entier	3-15
A	MENEZES; OORSCHOT; VANSTONE: "HANDBOOK OF APPLIED CRYPTOGRAPHY, PASSAGE" CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, 1997, pages 551-552, XP002273115 BOCA RATON, FL, USA ISBN: 0-8493-8523-7 page 551, alinéa 13.3.1 - page 552	1,2
A	PATARIN J ; GOUBIN L ; COURTOIS N: "Improved algorithms for isomorphisms of polynomials" ADVANCES IN CRYPTOLOGY - EUROCRYPT '98. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, 4 juin 1998 (1998-06-04), pages 184-200, XP002273116 Espoo, Finland ISBN: 3-540-64518-7 le document en entier	3-15